UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,181	03/02/2002	Chia-Chi Feng	1007-022	4754

22898 7590 05/16/2005

THE LAW OFFICES OF MIKIO ISHIMARU
1110 SUNNYVALE-SARATOGA ROAD
SUITE A1
SUNNYVALE, CA 94087

EXAMINER	
DAFTUAR, SAKET K	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,181	FENG, CHIA-CHI	
	Examiner	Art Unit	
	Saket K. Daftuar	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/02/2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 March 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 090117505, filed on July 18, 2001 in Taiwan, Republic of China.

Drawings

3. The drawings are objected to under 37 CFR 1.83(a) because they fail to show transmission system 2, transmission system 7, and retrieval transmission module 51, 61 in Fig. 3, Fig4 and Fig 5, respectively, as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary

to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The disclosure is objected to because of the following informalities: Applicant failed to indicate processing center 3 in Fig. 6 when describing detailed invention. It is suggested to declare "Fig. 6 is a flowchart showing the steps involved, in conjunction with Fig. 5, in an electronic file transmission method..." The repetition of same error found in, later, detailed description of Fig 7, Fig 8, Fig 9 and Fig 10.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 3, 6, 8,9, 11 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Hillegass et al. U.S. Patent Application Publication Number US 2002/0010681 (hereinafter Hillegass).

As per claim 1, Hillegass discloses an electronic file transmission method for use with an electronic file transmission system including a file processing center [a vendor, license server (abstract)], a transmission network [server software running provided by license provider (abstract)] and at least one file reading device [player software operating on the user's computer (abstract)], wherein the file reading device is provided with a hardware serial number; the electronic file transmission method comprising the steps of:(1) performing a file transmission process, allowing an electronic file to be symmetrically encrypted with the hardware serial number [The product license is also limited to a particular user by containing a user ID (Hillegass, Paragraph 0033)] of the file reading device and transmitted between the file processing center and the file reading device through the transmission network [Digitally encrypted communication streams keep certain communication between the producer software, the license provider, and the player software confidential (Hillegass, Paragraph 0009)], whereby the encrypted file is capable of being symmetrically decrypted only by using the same hardware serial number for file retrieval at the file processing center or the file reading device [Encrypted file having decryption key specific for that product file. Product license can be obtain by interaction

between the player software and the license server (Hillegass, Paragraph 0032)], and the decrypted file is again symmetrically encrypted with the same hardware serial number for file storage [Fig 4, encryption key has been received from the registration server (Hillegass, Paragraph 0040) After the encryption is finished, the product software saves the file (Hillegass, Paragraph 0041)]; and (2) ending the file transmission process between the file processing center and the file reading device [After encryption is finished , the product software saves file and then process of creating file is complete (Hillegass, Paragraph 0042)].

As per claim 3, Hillegass discloses (1-2-1) requesting via the file reading device for downloading an electronic file from the file processing center; [The player software submits to the license server a request for a new product license (Hillegass, Paragraph 62)] retrieving a hardware serial number corresponding to the file reading device via the file processing center from a database thereof, and [The license provider also operates a database, which stores information about vendors, users, product files, and licenses; and a license server, which is used to control the licensing of product files (Hillegass, Paragraph 0026)] symmetrically encrypting the electronic file with the hardware serial number via an encryption/decryption module of the file processing center, allowing the encrypted file to be transmitted from the file processing center to the file reading device through the transmission network [[This submission includes the appropriate product ID, the user ID of the user, the vendor ID found in file the

encrypted session key, and any changes to the user profile made by user (Hillegass, Paragraph 62)];(1-2-2) upon receiving the encrypted file from the file processing center via the file reading device, symmetrically decrypting the encrypted file via a retrieval/transmission module of the file reading device by using the same hardware serial number as for file encryption, and displaying [Displaying the images whenever the file is played (Hillegass, Paragraph 0024)] the decrypted file on a screen of the file reading device [Examiner considers, Hillegass, Fig 7 for transmitting the encrypted file and decrypted the encrypted file using the product license that includes user id as well]; (1-2-3) symmetrically encrypting the decrypted file with the same hardware serial number via the retrieval/transmission module of the file reading device for file storage; and [Examiner considers, Hillegass, Fig 7 for storing the file after being decrypted the encrypted file]; (1-2-4) determining via the file reading device if to continue downloading another electronic file from the file processing center, wherein if file downloading is continued, the step (1-2-1) is returned; or else, file downloading is ended [Whether a valid product license is determined to exist or whether to purchase a new product license (Hillegass, Paragraph 0052)].

As per claim 6, Hillegass discloses the transmission network is Internet or intranet [available over the Internet (Hillegass, Paragraph 0004)].

As per claim 8, Hillegass discloses a method of (1) performing a registration initiation process, so as to allow the file processing center to obtain the hardware serial number of the file reading device [When a new product is entered into database, the license provider creates a product ID and stores this ID with the other product information in database (Hillegass, Paragraph 0046)]; 1) performing a file transmission process, allowing an electronic file to be symmetrically encrypted with the hardware serial number [The product license is also limited to a particular user by containing a user ID (Hillegass, Paragraph 0033)] of the file reading device and transmitted between the file processing center and the file reading device through the transmission network [Digitally encrypted communication streams keep certain communication between the producer software, the license provider, and the player software confidential (Hillegass, Paragraph 0009)], whereby the encrypted file is capable of being symmetrically decrypted only by using the same hardware serial number for file retrieval at the file processing center or the file reading device [Encrypted file having decryption key specific for that product file. Product license can be obtain by interaction between the player software and the license server (Hillegass, Paragraph 0032)], and the decrypted file is again symmetrically encrypted with the same hardware serial number for file storage [Fig 4, encryption key has been received from the registration server (Hillegass, Paragraph 0040) After the encryption is finished, the product software saves the file (Hillegass, Paragraph 0041)]; and (2) ending the file transmission process between the file processing

center and the file reading device [After encryption is finished , the product software saves file and then process of creating file is complete (Hillegass, Paragraph 0042)].

As per claim 9, Hillegass discloses the steps of (1-1) establishing connection via the transmission network between the file processing center and the file reading device, so as to allow the file processing center to transmit a public key thereof to the file reading device [encryption key received from the registration server (Hillegass, Paragraph 0041)]; (1-2) upon receiving the public key from the file processing center via the file reading device, encrypting the hardware serial number of the file reading device via a retrieval/transmission module of the file reading device by using the public key and an encryption method of an asymmetrically unidirectional function, and transmitting the encrypted hardware serial number to the file processing center via the transmission network; and [encrypting the session key using a public key associated with the remote license generator (Hillegass, claim 31 and Paragraph 0061)] (1-3) upon receiving the encrypted hardware serial number from the file reading device via the file processing center, decrypting the encrypted hardware serial number via an encryption/decryption module of the file processing center by using a private key thereof and a decryption method of an asymmetrically unidirectional function, so as to obtain the unencrypted hardware serial number of the file reading device and store the hardware serial number in a database of

the file processing center [The license server will then decrypt the session key with its private key (Hillegass, Paragraph 63)].

As per claim 11, claim 11 falls under the same limitation of claim 3. Therefore, claim 11 has been rejected under same rationale.

As per claim 14, claim 14 falls under the same limitation of claim 6. Therefore, claim 14 has been rejected under same rationale.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2,4,5,7,10,12,13,15,and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hillegass et al. U.S Patent Application Publication Number 2002/0010681 (hereinafter Hillegass) as applied above in view of Obrador et al. U.S Patent Application Publication Number 2002/0049660 (hereinafter Obrador).

As per claim 2 and 10, Hillegass discloses the steps of (1-1) determining if the file reading device requests for downloading an electronic file from the file processing center [requests to purchase access to the product file (Hillegass, Claim 36)]; and (1-2) for file downloading, symmetrically encrypting the electronic file with the hardware serial number of the file reading device [The product license is also limited to a particular user by containing a user ID (Hillegass, Paragraph 0033)] via the file processing center, and transmitting the encrypted file from the file processing center to the file reading device, where the encrypted file is decrypted by using the same hardware serial number as for file encryption [Examiner considers, Hillegass, Fig 7 for transmitting the encrypted file and decrypted the encrypted file using the product license that includes user id as well].

Hillegass explicitly discloses a reading device, an encryption and decryption module, symmetrically encrypted on downloaded file with public key, decrypt downloaded encrypted file with private key and store the encrypted file in the database.

However, Hillegass failed to disclose uploading an encrypted electronic file to the file processing center.

Obrador teaches uploading (1-3) for file uploading, symmetrically encrypting the electronic file with the hardware serial number via the file reading device [Upload the identified data files to the server for storage (Obrador, Paragraph 0049)], and transmitting the encrypted file from the file reading device to the file processing center [Using conventional FTP file transfer to the Server by the participant (Obrador, Paragraph 0049)], where the encrypted file is decrypted by using the same hardware serial number as for file encryption.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to provide secure licensing digital works by symmetrically encrypting the file and later, decrypting an encrypted file while downloading, of Hillegass, and uploading as taught by Obrador, in order to efficiently limit the digital license.

As per claims 4 and 12, Hillegass explicitly discloses symmetrically encrypted on downloaded file with public key, decrypt downloaded encrypted file with private key and store the encrypted file in the database.

However, Hillegass failed to disclose uploading an encrypted electronic file to the file processing center. Hillegass doesn't explicitly disclose the file reading device for uploading a symmetrically encrypted electronic file to the processing center.

Obrador teaches (1-3-1) requesting via the file reading device for uploading an electronic file to the file processing center [Upload the identified data files to the server for storage (Obrador, Paragraph 0049)], and symmetrically encrypting the electronic file with the hardware serial number of the file reading device via an encryption/decryption module of the file reading device, allowing the encrypted file to be transmitted from the file reading device to the file processing center through the transmission network [Using conventional FTP file transfer to the Server by the participant (Obrador, Paragraph 0049)]; (1-3-2) upon receiving the encrypted file from the file reading device via the file processing center, retrieving a hardware serial number corresponding to the file reading device, and symmetrically decrypting the encrypted file via an encryption/decryption module of the file processing center by using the retrieved hardware serial number, [Once the exchange server sends information to and receives information from multiple participants and when all these participants has registered and posted their information, the vendors further upload data files. The exchange server then retrieve information from the relational database and matches all attributes of the available services (Obrador, Paragraph 0050)] so as to obtain the file content; (1-3-3) determining via the file reading device if to continue uploading another electronic file to the file processing center, wherein if file uploading is continued, the step (1-3-1) is returned; or else, file uploading is ended [Once the exchange server matches

service returned by the database, it is returned to the original vendor to determine further action (Obrador, Paragraph 0050)].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to provide secure licensing digital works by symmetrically encrypting the file and later, decrypting an encrypted file while downloading, of Hillegass, and uploading as taught by Obrador, in order to efficiently limit the digital license.

As per claims 5 and 13, Hillegass explicitly discloses a reading device, an encryption and decryption module, symmetrically encrypted on downloaded file with public key, decrypt downloaded encrypted file with private key and store the encrypted file in the database.

However, Hillegass failed to disclose uploading an encrypted electronic file to the file processing center. Hillegass doesn't explicitly disclose the file reading device for uploading a symmetrically encrypted electronic file to the processing center.

Obrador teaches the file processing center is a digital information server for providing electronic files to be downloaded by the file reading device and storing electronic files uploaded from the file reading device. [Upload identified

data files to the server for storage and further processing (Obrador, Paragraph, 0049)]

Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to provide secure licensing digital works by symmetrically encrypting the file and later, decrypting an encrypted file while downloading, of Hillegass, and uploading as taught by Obrador, in order to efficiently limit the digital license.

As per claim 7 and 15, Hillegass explicitly discloses a reading device is a personal computer.

However, Hillegass failed to disclose file reading device is personal digital assistant or an electronic book reader. Hillegass doesn't explicitly disclose the file reading device for uploading a symmetrically encrypted electronic file to the processing center by using personal digital assistant or an electronic book reader.

Obrador also teaches the file reading device is a personal computer and a personal digital assistant or an electronic book reader [permit a transmission to be made to another kind of WAP enabled device, such as a PDA (Obrador, Paragraph (0090)].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to provide secure licensing digital works by symmetrically encrypting the file and later, decrypting an encrypted file while downloading, of Hillegass, uploading as taught by Obrador and download or upload encrypted electronic file by using personal digital assistant or electronic book reader, in order to efficiently limit the digital license.

As per claim 16, Hillegass discloses at least one file reading device having a hardware serial number [at least one product license having a product identifier (Hillegass, claim 39], for symmetrically decrypting a downloaded encrypted file by using the hardware serial number of the file reading device, wherein the decrypted file is again symmetrically encrypted with the same the hardware serial number by the file reading device for file storage; [Encrypted file having decryption key specific for that product file. Product license can be obtain by interaction between the player software and the license server (Hillegass, Paragraph 0032) Examiner considers, Hillegass, Fig 7 for storing the file after being decrypted the encrypted file], a database for storing the hardware serial number of the file reading device; and [The license provider also operates a database, which stores information about vendors, users, product files, and licenses; and a license server, which is used to control the licensing of product files (Hillegass, Paragraph 0026)],an encryption/decryption module, for asymmetrically decrypting an encrypted hardware serial number from the file

reading device by using a private key of the file processing center, so as to obtain the unencrypted hardware serial number and store the hardware serial number in the database; [The license server will then decrypt the session key with its private key (Hillegass, Paragraph 63)], and a transmission network for connecting the file processing center to the file reading device.

Hillegass failed to disclose uploading an encrypted electronic file to the file processing center from the file reading device. Hillegass doesn't explicitly disclose the file reading device for uploading a symmetrically encrypted electronic file to the processing center. However, he suggested that the combinations of features and elements are possible within the scope of the present invention.

Obrador teaches uploading (1-3) for file uploading, symmetrically encrypting the electronic file with the hardware serial number via the file reading device [Upload the identified data files to the server for storage (Obrador, Paragraph 0049)], and transmitting the encrypted file from the file reading device to the file processing center [Using conventional FTP file transfer to the Server by the participant (Obrador, Paragraph 0049)], where the encrypted file is decrypted by using the same hardware serial number as for file encryption.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to provide secure licensing digital works by symmetrically encrypting the file and later, decrypting an encrypted file while downloading, of Hillegass, uploading as taught by Obrador and download or upload encrypted electronic file by using personal digital assistant or electronic book reader, in order to efficiently limit the digital license.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying P.T.O 892.

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. Failure to respond within the period for response will result in **ABANDONMENT** of the applicant (See 35 U.S.C 133, M.P.E.P 710.02,71002 (b)).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Saket K. Daftuar** whose telephone number is **571-272-8363.** The examiner can normally be reached on 8:30am-5:00pm M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Zarni Maung** can be reached on **571-272-3939**. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Saket Daftuar
Art Unit 2151
May 6, 2005

ZARNI MAUNG
SUPERVISORY PATENT EXAMINER